陷门不可识别的密文检索方案

杜瑞忠[1,2] 谭艾伦[1,2] 田俊峰[1,2]

[1]（河北大学网络空间安全与计算机学院 河北保定 071002）

[2]（河北省高可信信息系统重点实验室 河北保定 071002）

（drzh@hbu.edu.cn）

Unrecognizable searchable encryption scheme

Du Ruizhong[1,2], Tan Ailun[1,2],and Tian Junfeng[1,2]

[1]（*Cyberspace Security and Computer College, Hebei University, Baoding 071002*）

[2]（*Key Laboratory on High Trusted Information System in Hebei Province, Baoding 071002*）

Abstract Attribute-based encryption has been widely used in ciphertext retrieval in the cloud environment, but the flexible control of attributes and the privacy of trapdoors are still difficult problems to be solved in ciphertext retrieval. In order to solve the above problems, a ciphertext retrieval scheme with unrecognizable trapdoors is proposed. Aiming at the problem that only attributes are allowed to pass through in the traditional access strategy, a denial of access strategy is proposed. By using the calculation of data set, user attributes are controlled in two directions in the cloud server, providing more flexible access control. The random number is introduced in the trapdoor calculation process, so that the different trapdoors generated by the same keyword at different times, which can effectively resist the cloud server and the external attacker's guessing attack on the keyword. The safety of the scheme is proved, the system security can be statuted to the difficult problem of BDBH, and the theoretical analysis and experimental analysis of the scheme are carried out. After repeated experiments on the real data set, the results show that the scheme has higher security and retrieval. effectiveness.

Key words attribute-based encryption; unrecognizable trapdoor; two-way access strategy; ciphertext search

摘要 属性基加密在云环境下的密文检索中已经广泛运用，但属性的灵活控制以及关键字陷门的隐私安全仍然是密文检索中亟待解决的困难问题．为了解决上述问题，提出陷门不可识别的密文检索方案．针对传统访问策略中只允许属性通过的问题，提出拒绝访问策略，利用数据集合的计算，在云服务器中实现双向控制用户属性，提供更加灵活的访问控制．在陷门计算过程中引入随机数，使得同一个关键字在不同时刻产生的陷门互不相同，可有效的抵御云服务器以及外部攻击者对关键字的猜测攻击．对方案进行安全证明，其系统安全性可规约到 BDBH 困难问题，同时对方案进行了理论分析以及实验分析，经过在真实数据集上进行反复实验，结果表明该方案具有更高的安全性与检索效率．

关键词 属性基加密；不可识别陷门；双向访问策略；密文检索

中图法分类号 TP309

云存储是当下一种主流的在线存储方式，在免去了用户在本地存储的硬件开销与管理开销的同时，使得数据脱离了用户的物理控制，因此数据的安全受到巨大威胁．为了解决云存储的数据安全问题，一般采用数据加密的方式，但是加密后的数据在云服务器中会导致检索困难的问题．

为了增强数据在服务器上的安全性，song 等人[1]首次提出了一对一机制的可搜索加密方案．为了满足多用户的环境，Boneh 等人[2]提出基于公钥密码的可搜索加密方案(PEKS)，并证明了公钥可搜索加密体系是语义安全的，但是不能抵御关键字猜测攻击．关键字猜测攻击是可搜索加密中的一种攻击方式，主要针对上传的陷门进行统计分析，由于同一个关键字的陷门是相同的，一些常用关键字的陷门会被大量的上

基金项目：国家自然科学基金项目（61170254, 60873203）；河北省自然科学基金项目（F2016201244，F2018201153）；河北省高等学校科学技术研究基金项目（ZD2016043）；河北省物联网数据采集与处理工程技术研究中心基金项目（河北 065201）

This work was supported by the National Natural Science Foundation of China (61170254, 60873203), the Natural Science Foundation of Hebei Province (F2016201244，F2018201153), the Science and Technology Research Project in Colleges and Universities of Hebei Province (ZD2016043), and the Hebei Engineering Technology Research Center for IoT Data Acquisition & Processing, North China Insitute of Science and Technology (Hebei 065201).

传，导致服务器或攻击者能够猜测到这个陷门的含义．为了抵御关键字猜测攻击，Fang 等人[3]提出一种可以抵御没有随机预言的关键字攻击的公钥加密方案，但是服务器的内部攻击是该方案的软肋．就此问题，Shao 等人[4]提出一种能够抵御服务器进行关键字猜测攻击的方案．关键字猜测攻击最好的防御方式就是让关键字陷门变得不可识别，同一关键字每次产生的陷门不同．关键字隐私保护主要是陷门的隐私安全性，如何构建安全的陷门是密文检索方向的一个研究难点．

为了让密文检索更加的灵活与高效，属性基加密（Attribute-basedencryption，ABE）[5]被提出，其中基于密文策略的属性基加密方案（ciphertext-policyAttribute-basedencryption,CP-ABE）[6]可以在密文中镶嵌访问控制策略，能够灵活的控制访问的用户属性，但是也带来了属性撤销的困难问题．在云环境下的数据呈现动态、海量等特点，基于属性基加密的密文检索方案需要能够高效的对属性与策略进行修改．Piretti 等人[7]提出属性撤销方案，通过对每个属性设定有效期，授权机构周期性地更新属性版本，通过撤销某个属性的最新版本以此达到用户属性撤销的目的．

在基于属性的密文检索方案一般存在三个方面的问题：安全问题、精度问题、效率问题．为了解决安全问题，Hur 等人[8]提出一种具有属性和用户撤销能力的 CP-ABE 方案，该方案增强了用户访问控制的前向安全和后向安全，同时具有属性级别的属性撤销能力．安全问题不仅仅是方案中的撤销安全问题，用户的隐私安全也需要考虑．为此，Li 等人[9]提出云存储中可撤销属性的 CP-ABE，其中访问结构部分隐藏，使得接收者不能从密文中提取敏感信息．为保护用户的隐私，Ma 等人[10]提出基于隐私保护的 CP-ABE 方案，该方案不仅实现了属性的撤销，还能够有效的保护用户隐私．

为了提高撤销的精度，Yang 等人[11]提出一种云存储环境下支持细粒度属性撤销的属性基加密方案，该方案不需要服务器支持任何协作的访问控制，数据拥有者也不需要实时在线，但是该方案只是在随机预言机下证明其安全性．Zu 等人[12]提出一种云存储环境下具有有效撤销能力的 CP-ABE 方案，该方案的访问结构采用了 LSSS 模式，具有极强的表现能力．为了更细粒度的访问，Sun 等人[13]的方案利用 CP-ABE 和代理重加密技术实现了文件级别的访问授权且支持数据用户的属性撤销．Cui 等人[14]提出更高精度的密文检索方案 ABE-EAKS，方案能够实现对云中加密数据的细粒度访问控制．

在撤销效率方面，Xue 等人[15]提出了一个基于 0-1 编码的密文可比属性基加密方案，提出基于具有 0 编码和 1 编码概念的子属性的生成和管理的有效构造方法，并且存储和通信以及计算开销被大量减少．由于外包计算能够大量的减少用户的在线计算成本，因此，chen 等人[16]提出在线/离线密文策略属性基可搜索加密，利用离线状态下的预处理外包解密，降低了用户的在线计算成本，同时提高了效率．为了减少外包解密的计算开销，zhao 等人[17]提出一个恒定密文大小的属性基加密方案，该方案的密文大小恒定，不仅提高了外包计算效率，系统整体也变得极为高效．

密文检索的研究越来越多元化，Qian 等人[18]提出一种云环境下多授权中心的 CP-ABE 方案，该方案撤销属性过程中采用重加密技术更新密文，多授权中心能够有效地提高方案的整体效率．广播加密是典型的一对多模式，Canard 等人[19]将广播加密与属性基加密结合起来，形成一种新的秘密分享方式，适用于一对多的可搜索加密模式．liang 等人[20]将确定性删除与属性基加密结合在一起，提出一个支持撤销且能够证明的属性基密文检索方案．

针对现有方案中陷门安全性和属性细粒度访问的问题，提出一种陷门不可识别的密文检索方案(U-ABE)．该方案实现了不可识别陷门的构建，同时引入了拒绝访问策略，对属性的控制更加灵活．主要的工作如下：

（1）为解决陷门安全问题，利用双线性映射的双线性，加入随机数，构造动态的陷门，并证明了陷门的不可识别性．

（2）为了提高访问策略对属性的灵活控制，引入拒绝访问策略，与允许访问策略双向控制访问属性．撤销时可以通过上传拒绝访问策略撤销，实现双向的撤销方式．

（3）对方案进行安全性分析，证明方案满足关键字隐私安全，同时系统安全性可规约到 BDBH 困难问题．对方案进行理论分析与实验分析，结果表明方案具有较高的效率．

1 预备知识

1.1 双线性对

假设群 G 与群 G_T 是阶为素数 p 的循环群，g 是群 G 的生成元，存在双线性映射 $e:G\times G\rightarrow G_T$，并满足以下性质：

1）双线性：对任意的 x，y∈G，a，b∈G_T，存在 $e(x^a, y^b)=e(x^b, y^a)=e(x, y)^{ab}$．

2）非退化性：存在 g∈G，使 e(g，g)≠1．

3）可计算性：对所有的 x，y∈G，存在有效的算法计算 $e(x, y)$．

1.2 判定性双线性 Diffie-Hellman 假设

设群 G_1，G_2 及映射 e：$G_1\times G_1\rightarrow G_2$，$g$ 是群 G_1 的生成元，随机生成 a，b，c，$z\leftarrow_R Z_p$，生成两个五元组 $T_0=(g, A=g^a, B=g^b, C=g^c, Z=e(g, g)^z)$与 $T_1=(g, A=g^a, B=g^b, C=g^c, Z=e(g, g)^{abc})$．将两个五元组记为：

$$P_{BDH}=\{(g, g^a, g^b, g^c, e(g, g)^{abc})\}$$

$$R_{BDH}=\{(g, g^a, g^b, g^c, e(g, g)^z)\}$$

DBDH 假设：没有多项式时间的敌手，能以不可忽略的优势 ε 区分五元组 P_{BDH} 与 R_{BDH}．

1.3 文中符号列表

方案中的符号含义如下所示：

B：加密参数

Bi：解密参数

t_1：允许访问策略

t_2：拒绝访问策略

T_1：加密后的允许访问策略

T_2：加密后的拒绝访问策略

CT：密文，包括（C_m，C_k）

V：版本信息

ϕ：关键字索引

w：数据关键字集合

w_i：检索关键字集合

Sk_a：属性私钥集

T_w：关键字生成的陷门

p：匹配信息

SK：属性参数

2 系统模型和安全模型

2.1 系统模型

方案的系统模型如图 1 所示，方案中包括四个实体：数据拥有者（DO，Data owner）、云服务器（CS，Cloud sever）、数据使用者（U，User）、属性权威（AA，Attribute authority）．

1）属性权威．假定属性权威是可信的，属性权威的主要任务如下：生成属性的随机表格、对数据拥有者上传的策略进行加密以及计算加密参数；根据表格对数据使用者上传的属性进行计算，得到属性私钥及解密参数．

2）数据拥有者．DO 的主要任务如下：使用传统对称加密对数据进行加密；加入随机数的方法生成不可识别的索引；与属性权威进行数据交互，得到访问策略．

3）数据使用者．U 的主要任务如下：生成不可识别的随机陷门，与云服务器进行数据交互，得到服务器返回的版本号，将版本号与自身属性上传给属性权威，属性权威经过计算，返回属性私钥与解密参数．然后上传属性私钥到云服务器，服务器验证后返回密文．

4）云服务器．云服务器的主要任务如下：接收数据用户上传的陷门，下发密文版本号给数据用户；接收数据用户上传的属性私钥，匹配运算后下发密文给数据用户．

2.2 方案定义

1）$Setup(1^{\lambda})\rightarrow(Par, T)$：给定安全参数 λ，由可信的属性权威运行算法，输出公开参数 Par，以及随机属性表格 T，其中随机属性表格由属性权威(AA)私有，并且定时更新．

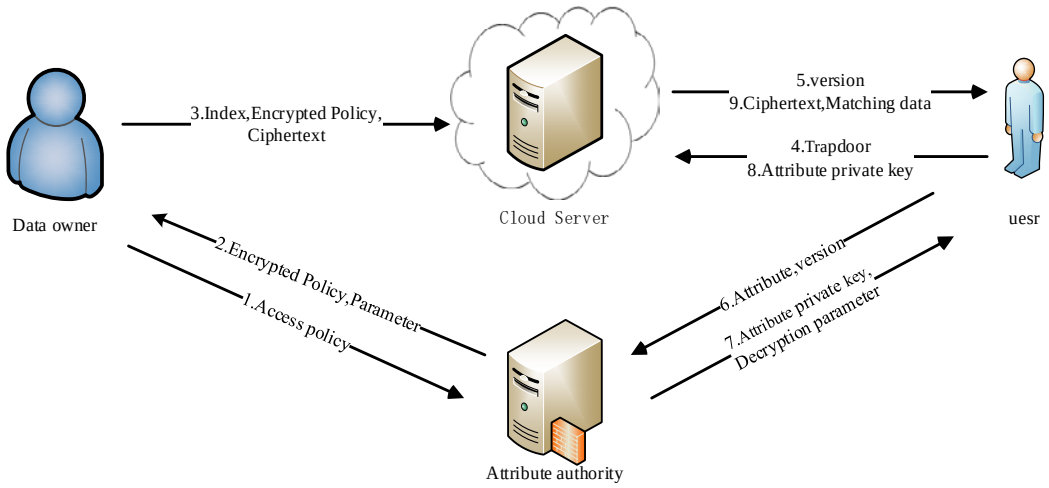


Fig1 system model diagram

图 1 系统模型图

2）$EncT(t_1, t_2, pp)\rightarrow(T_1, T_2, B)$：该算法由属性权威运行，$t_1$ 是数据拥有者上传给属性权威的允许访问策略集合，t_2 是数据拥有者上传给属性权威的拒绝访问策略集合；pp 是属性权威查询 t_1，t_2 集合中的属性在表格中定位的坐标．t_1，t_2 加密后得到密文状态的双向访问策略 T_1，T_2；pp 加密以后得到加密参数 B，并且嵌入加密的版本信息 V；属性权威将得到的密文数据回传给数据拥有者．

3）$Enc(m, k, w, B, par)\rightarrow(CT, \varphi)$：该算法由数据拥有者运行，$m$ 是明文数据，k 是对明文对称加密的密钥；w 是数据拥有者数据中包含的关键字集合；B 是加密参数．得到密文 CT，密文 CT 包含两个密文，一个是 C_m，它是明文 m 对称加密后得到的密文；另一个是 C_k，它是对密钥 k 加密后得到的密文．φ 是由关键字集合 w 加密后得到的索引．

4）$Trap(w_i, par)\rightarrow T_{wi}$：该算法由用户运行，$w_i$ 是用户查询的关键字．计算以后得到关键字陷门 T_{wi}，上传给云服务器用以检索．

5）$KeyGen(att, V)\rightarrow SK$：该算法由属性权威运行，$att$ 是由用户上传的属性，V 是版本信息，生成属性参数 SK．

6）$Search(T_1, T_2, \varphi, T_w, SK_a)\rightarrow 1\ or\ 0$：服务器运行该算法进行匹配检索，该算法在系统中分为两个阶段，第一阶段进行关键字检索，得到版本信息 V；第二阶段进行属性与访问策略匹配，属性必须不与拒绝访问策略中的属性集合有交集，同时包含允许访问策略中的属性集合．当两个阶段都满足要求，服务器下发密文 CT 给用户．

7）$Dec(CT, P, B_i)\rightarrow m$：该算法由用户运行，输入密文 CT，匹配信息 P，以及解密参数 B_i．通过计算得到明文 m．

2.3 安全模型

通过定义关键字隐私安全游戏和判定性双线性 Diffie-Hellman 假设困难问题规约证明来构造安全模型．

2.3.1 关键字隐私安全游戏

如果不存在敌手 A 能够在概率多项式时间内从密文关键字或陷门值推断出关键字明文信息，则关键字的隐私安全可以得到保证．按以下定义关键字隐私安全游戏．

1）初始化．给定安全参数 λ，挑战者 C 执行初始化算法 $Init(1^{\lambda})$，生成公共参数 par．

2）阶段 1．敌手 A 多次运行陷门生成算法．

3）挑战．挑战者 C 从关键字空间随机选取关键字 W'，然后执行算法 $Trap(w_i, par)$，最后将陷门 T_{wi} 发送给敌手 A．

4）猜测．敌手 A 查询了 τ 个不同的关键字后，敌手 A 输出一个关键字 W'，如果 $W=W'$，则敌手 A 在安全游戏中获胜．

方案是支持关键字安全隐私的，敌手 A 在安全游戏中获胜的概率最多为 $\frac{1}{|\Psi|-n}+\varepsilon$．其中，$n$ 表示关键字集的个数，ε 表示在安全参数 λ 下可以忽略的概率，Ψ 表示关键字的空间．

2.3.2 判定性双线性 Diffie-Hellman 假设困难问题规约证明

如果存在敌手 A 能够在多项式时间内以优势 δ 破解方案，则敌手 A 能在多项式时间内以优势 δ 解决 DBDH 困难问题．按以下定义判定性双线性 Diffie-Hellman 假设困难问题规约证明．

1）初始化．给定群组 G_1，G_2 及映射 e:$G_1\times G_1\rightarrow G_2$．挑战者随机生成 a，b，c，$z\leftarrow_R Z_p$，生成两个五元组 T_0，T_1．$T_0=(g, A=g^a, B=g^b, C=g^c, Z=e(g, g)^z)$，$T_1=(g, A=g^a, B=g^b, C=g^c, Z=e(g, g)^{abc})$．

2）阶段 1．敌手 A 多次运行加密算法．

3）挑战．挑战者 C 随机选取明文 m．并要求 m 在阶段 1 未被查询，生成密文 C，并将密文传给敌手 A．

4）猜测．敌手 A 对密文 C 进行分析解密，如果敌手能够解出密文 C 且得到正确的明文 m，则敌手在游戏中获胜．

5）证明．敌手 A 能够对密文进行解密，则敌手 A 也能解决判定性双线性 Diffie-Hellman 假设困难问题．

3 系统描述

1）初始化阶段

$Setup(1^{\lambda})\rightarrow(Par, T)$：给定安全参数 λ，可信的属性权威运行算法，输出双线性映射参数 (G_1,G_2,e,p,g)，其中，G_1 和 G_2 是阶为素数 q 的乘法循环群，g 是 G_1 的生成元，双线性映射 e：$G_1\times G_1\rightarrow G_2$，然后生成随机数 $a,b\in Z_q$，然后定义哈希函数 H:$\{0,1\}^*\rightarrow G_1$，最后输出公共参数 par．

$$par=(a, b, g, g^a, g^b, G_1, G_2, e, q, H)$$

属性权威生成表格 T，为属性权威私有，表格 T 中放入各种属性，如表 2 所示．属性的坐标在计算中代表这个属性，坐标是由随机数构成的，且坐标数据定时更换．表格的版本信息 v 经过属性权威加密以后得到密文的版本信息 V，当表格 T 中的坐标数据更换时，属性权威就会计算得到新的版本信息

Table 1 attribute list instance

表 1 属性列表实例

X / Y	x_1	x_2	x_3	x_4	x_5	…..	x_n
Y_1	A_{11}	A_{21}	A_{31}	A_{41}	A_{51}	…	A_{n1}
Y_2	A_{12}	A_{22}	A_{32}	A_{42}	A_{52}	…	A_{n2}
Y_3	A_{13}	A_{23}	A_{33}	A_{43}	A_{53}	…	A_{n3}
Y_4	A_{14}	A_{24}	A_{34}	A_{44}	A_{54}	…	A_{n4}
Y_5	A_{15}	A_{25}	A_{35}	A_{45}	A_{55}	…	A_{n5}
……	…	…	…	…	…	…	…
Y_n	A_{1n}	A_{2n}	A_{3n}	A_{4n}	A_{5n}	…	A_{nn}

2）加密阶段

EncT(t_1，t_2，*pp*)→(T_1，T_2，*B*)：属性权威接收数据拥有者上传的允许访问策略 t_1 和拒绝访问策略 t_2，然后在属性表格 *T* 中查找，得到坐标数据 *pp*.

$$pp=[\{(x_1,y_1),(x_2,y_2),\ldots,(x_i,y_i)\}_{t_1}、$$
$$\{(x_1,y_1),(x_2,y_2),\ldots,(x_u,y_u)\}_{t2}\};1\le i,u\le n]$$

属性权威用 *pp* 中的坐标数据进行计算得到 T_1，T_2，以及加密参数 *B*.

$$T_1=\{(g^{x_1},g^{y_1}),(g^{x_2},g^{y_2}),\ldots,(g^{x_i},g^{y_i})\}$$
$$T_2=\{(g^{x_1},g^{y_1}),(g^{x_2},g^{y_2}),\ldots,(g^{x_u},g^{y_u})\}$$
$$B=\prod_1^i H(x_i^{y_i})$$

Enc(*m*，*k*，*w*，*B*，*par*)→(*CT*，φ)：密文 *CT* 中包含密文 C_k 与 C_m，*CT*=(C_k，C_m)，数据拥有者对明文 *m* 进行对称加密，使用对称密钥 *k*，得到密文 C_m. 然后对密文 *k* 进行加密，首先生成一个随机数 $t\leftarrow Z_p$，然后计算：

$$C_k=\{e(g^a,g^b)t\bullet k,g^t,B^t\} \quad (1)$$

c 数据拥有者需要对数据中的关键字建立索引，关键字集合 $w=(w_1,w_2,\cdots,w_n)$，生成随机数集合 $R\leftarrow Z_p$，然后进行计算得到：

$$\varphi=\{(g^{t_1},w_1^{t_1}),(g^{t_2},w_2^{t_2}),\cdots,(g^{t_n},w_n^{t_n})\}$$

Trap(w_i，*par*)→T_w：该算法由用户运行得到关键字陷门，输入查询关键字集合 w_i，生成随机数集合 $P\leftarrow Z_p$，计算得到：

$$T_w=\{(g^{p_1},w_{i_1}^{p_1}),(g^{p_2},w_{i_2}^{p_2}),\cdots,(g^{p_n},w_{i_n}^{p_n})\}$$

KeyGen(*att*，*V*)→*SK*：用户与服务器进行第 1 阶段的数据交互以后，会收到云服务器下发的数据加密版本信息 *V*，用户将自身的属性 *att* 与版本信息 *V* 一起发送给属性权威 *AA*，属性权威 *AA* 将用户的属性 *att* 在对应版本 *V* 的表格 *T* 中查找对应的坐标数据，然后将坐标数据进行计算得到属性参数 *SK*.

$$SK=[\{e(g^{\alpha_1},g^{\beta_1}),H(\alpha_1^{\beta_1})\},\{e(g^{\alpha_2},g^{\beta_2}),$$
$$H(\alpha_2^{\beta_2})\},\cdots,\{e(g^{\alpha_n},g^{\beta_n}),H(\alpha_n^{\beta n})\}]$$

Search(T_1，T_2，φ，T_w，SK_a)→1 *or* 0：检索分为两个阶段.

阶段 1：用户向云服务器上传陷门 T_w，服务器将陷门与索引进行匹配计算，由于陷门中的关键字是一个集合，索引中的关键字也是一个集合，需要进行类似于集合相等的匹配. 计算：

$$e(g^{p_1},w_1^{t_1})=e(g^{t_1},w_{i_1}^{p_1})$$

如果等式成立，则证明 w_1 与 w_{i_1} 是同一关键字. 如果该等式不相等，则进行下一个关键字的计算，直到索引中的最后一个关键字. 服务器对匹配结果进行排序，然后将数据的加密版本信息 *V* 下发给用户.

阶段 2：用户在阶段 1 结束后收到服务器下发的版本信息 *V*，然后与属性权威进行数据交互，得到属性参数 *SK*，计算属性私钥 SK_a：

$$SK_a=\{e(g^{\alpha_1},g^{\beta_1}),e(g^{\alpha_2},g^{\beta_2}),\cdots,e(g^{\alpha_n},g^{\beta_n})\}$$

用户向服务器上传属性私钥 SK_a，云服务器进行属性与访问策略的匹配. 由于本方案中有两种访问策略，并且拒绝访问策略中包含的属性一定不能被用户属性私钥所包含，所以用户属性私钥需要先与拒绝访问策略 T_2 进行匹配，计算集合：

$$T_2\cap SK_a=\{(g^{x_1},g^{y_1}),(g^{x_2},g^{y_2}),\cdots,(g^{x_n},g^{y_n})\}$$
$$\cap\{(g^{x_{i_1}},g^{y_{i_1}}),(g^{x_{i_2}},g^{y_{i_2}}),\cdots,(g^{x_{i_n}},g^{y_{i_n}})\}$$

如果匹配结果非空集，则输出 0. 如果匹配结果为空集，则与允许访问策略 T_1 进行匹配. 计算集合：

$$T_1\cap SK_a=\{(g^{x_1},g^{y_1}),(g^{x_2},g^{y_2}),\cdots,(g^{x_n},g^{y_n})\}$$
$$\cap\{(g^{x_{\alpha_1}},g^{y_{\alpha_1}}),(g^{x_{\alpha_2}},g^{y_{\alpha_2}}),\cdots,(g^{x_{\alpha_n}},g^{y_{\alpha_n}})\}$$

当结果为 T_1 时，匹配成功，最后服务器输出 1，将密文 *CT* 以及属性匹配信息 *p* 下发给用户.

Dec(*CT*，*P*，B_i)→*m*：用户使用该算法对服务器

下发的密文 CT 进行解密，首先用户从匹配信息 p 中得到匹配成功的属性信息，然后计算解密参数 $B_i=\prod_j^n H(x_j^{y_j})$ 成一个随机数 $r\leftarrow Z_p$，计算得到：

$$\begin{aligned}&e(g^a,g^b)^t k\bullet\frac{e(g^r,B_i^t)}{e(g^{ba}B_i^r,g^t)}\\&=e(g^a,g^b)^t k\frac{e(g^r,B_i^t)}{e(g^{ba},g^t)e(B_i^r,g^t)}\\&=e(g^a,g^b)^t k\frac{e(g^r,B_i^t)}{e(g^{ba},g^t)e(B_i,g)^{rt}}\\&=e(g,g)^{abt}k\frac{e(g,B_i)^{rt}}{e(g,g)^{abt}e(B_i,g)^{rt}}\\&=k\end{aligned}\qquad(2)$$

然后通过对称解密算法，解出明文 m.

4 安全性分析

方案能够保证数据安全性，数据通过传统的对称算法进行加密，密钥 k 再次加密得到密文 C_k，只有用户的属性在满足访问策略的时候，才可以得到密文 C_k 并进行解密. 同时，能够保证关键字的安全性，由于关键字陷门是随机加密的，能够抵抗关键字猜测攻击. 此外，由于关键的密文 C_k 的构造是按照判定性双线性 Diffie-Hellman 假设困难问题中的四元组的构造方式来进行的，密文的安全性可以规约为判定性双线性 Diffie-Hellman 假设困难问题.

定理 1 基于一般的双线性群，方案在随机预言模型下是关键字隐私安全的.

证明：关键字陷门不会泄露关键字信息.

初始化：挑战者 C 生成随机数 a、b$\leftarrow_R Z_P$，公开参数 par=(a，b，g，g^a，g^b，G_1，G_2，e，q).

1）阶段 1：敌手选取关键字集合$(W_1,W_2,\cdots,W_n)$，发送给挑战者 C，挑战者输出关键字集合生成的陷门集合$(T_{w_1}, T_{w_2}, \cdots, T_{w_n})$，并发送给敌手 A.

2）挑战：挑战者 C 从关键字空间里随机选者关键字 W_0，且 W_0 没有在阶段 1 中被敌手 A 查询过. 然后选取随机数 p，运行 Trap(w_i，par)，计算 $T_{w_0}=(g^p,w_0^p)$ $T_{w_0}=(g^p,w_0^p)$，将 T_{w_0} 发送给敌手 A.

3）阶段 2：敌手 A 再次向挑战者发送关键字集合，与阶段 1 相同.

4）猜测：敌手 A 猜测关键字 W_0，在查询了 τ 个不同的关键字后，输出 W^*，如果 $W=W^*$，则敌手 A 赢得游戏.

证明：方案是支持关键字隐私安全的，由于关键字陷门在加密时引入了随机数，导致同一个关键字生成的陷门不同，可有效地抵御统计分析攻击. 敌手 A 在安全游戏中获胜的概率最多是 $\frac{1}{|\Psi|-n}+\varepsilon$. 其中，n 表示关键字集的个数，ε 表示在安全参数 λ 下可以忽略的概率，Ψ 表示关键字的空间.

定理 2 基于一般的双线性群，方案的安全性可以规约到判定性双线性 Diffie-Hellman 假设困难问题. 如果存在敌手 A 能够在多项式时间内以优势 δ 破解方案，则存敌手 A 能在多项式时间内解决 DBDH 困难问题.

证明：敌手 A 能在多项式时间内以优势 δ 攻破方案，那么敌手 A 也能在多项式时间内以优势 δ 解决判定性双线性 Diffie-Hellman 假设困难问题.

初始化：建立系统，生成安全参数 λ，然后运行算法 $Setup(1^\lambda)$，得到安全参数 $par=(a, b, g, g^a, g^b, G_1, G_2, e, q)$，以及系统中的加密参数 B.

阶段 1：敌手 A 多次运行加密算法.

挑战：挑战者 C 选取一个密钥 k，要求 k 在阶段 1 并没有被敌手 A 查询. 运行加密算法 $Enc(m, k, B, par)\rightarrow CT$，生成随机数 t，计算得到 $C_k=(e(g_1,g_2)^t\bullet k, g^t, B^t)$. 然后挑战者 C 将密文 C_k 发送给敌手 A.

猜测. 敌手 A 收到密文 C_k 以后，对密文进行分析解算. 然后敌手输出猜测的结果 k'，如果 $k=k'$，则敌手 A 赢得游戏. 如果敌手 A 能够对密文 C_k 进行正确解密，那么敌手 A 就能区分密文 C_k 中的 $e(g_1,g_2)^t$.

阶段 2：敌手 A 尝试判定性双线性 Diffie-Hellman 假设中的两种五元组.

初始化：敌手 A 多次运行算法计算两种五元组.

挑战. 挑战者 C 随机选择 a，b，c，$z\leftarrow_R Z_P$. 生成两个五元组，T_0 是随机五元组，$T_0=(g, A=g^a, B=g^b, C=g^c, Z=e(g, g)^z)$；$T_1$ 是 BDH 五元组，$T_1=(g, A=g^a, B=g^b, C=g^c, Z=e(g, g)^{abc})$. 挑战者 C 随机生成 $\mu\leftarrow_R\{0, 1\}$，若 $\mu=0$，则输出 T_0，若 $\mu=1$，则输出 T_1. 挑战者将得到的五元组发送给敌手 A.

猜测：敌手 A 接收到挑战者 C 发出的五元组 $T^*=(g, A=g^a, B=g^b, C=g^c, Z=e(g, g)^*)$进行分析，然后输出 μ'，如果 $\mu=\mu'$，则敌手 A 在游戏中获胜. 由上述所得，敌手 A 能够对密文中的 $e(g_1,g_2)^t$ 进行区分，然而密文中的 $e(g_1, g_2)^t=e(g, g)^{abt}$，也就是说敌手 A 能够对 $e(g, g)^{abt}$ 进行区分，则敌手 A 能够对挑战者 C 发送的五元组 $T^*=(g, A=g^a, B=g^b, C=g^c, Z=e(g, g)^*)$中的 $e(g, g)^*$进行区分. 因此，敌手 A 能够正确输出对 μ 的猜测值.

证明：敌手 A 能够对密文 C_k 进行解密，则敌手 A 能够解决判定性双线性 Diffie-Hellman 假设困难问题. 综上所述，方案的密文安全性可以规约到判定性双线性 Diffie-Hellman 假设困难问题.

5 性能分析

5.1 理论分析

在理论上，U-ABE 方案主要与其他几种方案做如下三个方面的对比：功能性、存储成本、通信成本. 同时在对比过程中的符号定义如下：|p|表示 Z_p 中数据元素的长度；|g|表示 G 中数据元素的长度；$|g_T|$表示 G_T 中数据元素的长度；$|C_k|$表示 Hur 方案中使用的密钥 KEK 的长度；n_c 表示与密文有关的属性个数；n_k 表示用户密钥中属性的个数；n_a 表示整个系统的属性个数.

5.1.1 功能分析

在表 2 中，将 U-ABE 方案与其他四个方案进行功能上的对比，各个方案的撤销机制都是立即撤销，U-ABE 与其他四个方案不同的地方在于撤销方向，由于 U-ABE 方案中加入了拒绝访问策略，所以在撤销的时候满足双向撤销. U-ABE 的访问策略采用的是 AND 模式，其他方案采用的是 Tree 或者 LSSS 模式，AND 模式的资源消耗更少，效率更高.

Table 2 Comparison of attribute revocation schemes

表 2 属性撤销方案功能对比

scheme	Access policy	Revocation mechanism	Security hypothesis	Revocation direction
scheme [8]	Tree	Immediate revocation	---	Forward revocation
scheme [18]	LSSS	Immediate revocation	q-parallel BDHE	Forward revocation
ABKS-UR[13]	Tree	Immediate revocation	BDBH	Forward revocation
AD-KP-ABE[20]	Tree	Immediate revocation	BDBH	Forward revocation
U-ABE	AND	Immediate revocation	BDBH	Two-way revocation

5.1.2 储存成本

在表3中，将U-ABE方案与方案[8]、[13]、[18]、[20]做了存储成本上的对比. 主要分为四个组成部分进行对比：属性权威、数据拥有者、云服务器、数据使用者. 在U-ABE方案中，属性权威的作用主要是生成属性表格、加密双向访问策略以及属性私钥. 属性权威的存储成本主要是随机数与表格，因此U-ABE方案中属性权威的存储成本计算为$(2n_a+1)|p|$，相比文献[8]来说，U-ABE方案更具优势. 在数据拥有者方面，方案中数据拥有者的主要工作是接收策略密文、生成索引以及加密数据，然后上传给云服务器. 由此计算得到数据拥有者的存储成本为$2|p|+|g|$，小于方案[8]、[18]、[13]、[20]的存储成本. 在云服务器方面，U-ABE方案中的云服务器的主要工作是接收数据拥有者上传的密文数据和数据使用者上传的检索信息及属性私钥、然后将两者进行匹配计算. 因此计算其存储成本为$(nc+nk)|g|+2|g_T|$，相比文献[8]、[13]、[20]，U-ABE方案降低了云服务器的存储成本. 最后是数据使用者方面，方案中数据使用者的工作是接收属性权威回传的属性参数SK，并计算得到属性私钥SK_a，以及生成陷门与解密. 因此，数据使用者的存储成本计算为$2n_k+|p|$，成本上小于文献[8]、[13]、[18]的方案.

Table 3 Comparison of storage cost of attribute revocation schemes

表 3 属性撤销方案储存成本对比

scheme	Attribute authority	Data owner	Cloud service	Data user
scheme [8]	$\|p\|+\|g\|$	$2\|g\|+\|g_T\|$	$(2n_c+1)\|g\|+\|g_T\|+(n_c\cdot n_u/2)\|C_k\|$	$(2n_k+1)\|g\|+\lg(n_u+1)\|C_k\|$
scheme [18]	$(4+n_a)\cdot\|p\|$	$(2+n_a)\|g\|+\|g_T\|$	$\|g_T\|+(3n_c+1)\|g\|$	$(2+n_k)\cdot\|g\|$
ABKS-UR[13]	---	$(3+n_a)\|g\|+\|g_T\|$	$\|g_T\|(n_c+2)+\|g\|(n_a+1)$	$2n_u\|g\|+\lg(n_u+2)$
AD-KP-ABE[20]	$2n_a\|p\|$	$n_c\|g\|+\|p\|$	$(n_c+n_k)\|g\|+\|g_T\|(n_c+2)$	$n_k\|p\|$
U-ABE	$(2n_a+1)\|p\|$	$2\|p\|+\|g\|$	$(n_c+n_k)\|g\|+2\|g_T\|$	$2n_k+\|p\|$

5.1.3 通信成本

在表 4 中，主要进行了通信成本上的理论分析，主要分为四条线路的数据传输成本，首先是 AA&U，在 U-ABE 方案中，属性权威与数据使用者之间主要是属性以及属性参数的传输，因此计算可得通信成本为 $2n_k+n_k|p|$. 其次是 AA&O，在 U-ABE 方案中，属性权威与数据拥有者之间主要是双向访问策略的明文密文以及加密参数的传输，由此通信成本可计算为 $4n_c+|p|$，相比方案[8]、[18]与[20]来说，通信成本大大降低. 在 CSP&U 过程中，U-ABE 方案中的服务器

与数据使用者有两次数据交互，主要是陷门、密文与属性私钥的传输，所以通信成本为$|p|+(n_k+1)|g_T|+n_c|g|$，优于其他四个方案．最后在 CSP&O 过程中，U-ABE 方案中的数据拥有者单方面上传密文数据给云服务器，因此通信成本计算为$(|g_T|+1)n_c+(n_c+1)|p|$.

Table 4 comparison of communication costs for attribute revocation schemes

表 4 属性撤销方案通讯成本对比

scheme	AA&U	AA&O	CSP&U	CSP&O
scheme [8]	$(1+2n_k)\|g\|$	$2\|g\|+\|g_T\|$	$(2n_c+1)\|g\|+\|g_T\|+(n_c\cdot n_u/2+\lg(n_u+1))\|C_k\|$	$2n_c\|g\|+(n_c+1)\|g_T\|$
scheme [18]	$4\|g\|+n_k\|g\|$	$2\|g\|+\|g_T\|+n_a\|g\|$	$\|g_T\|+(3n_c+1)\|g\|$	$\|g_T\|+(3n_c+1)\|g\|$
ABKS-UR[13]	---	---	$2\|p\|+(n_c+3)\|g_T\|+(n_c+4)/2$	$(2n_k+1)\|g\|+(n_c+1)\|g\|$
AD-KP-ABE[20]	$n_k\|p\|$	$n_c\|g\|+n_k\|g_T\|$	$\|p\|+(n_c+2)\|g\|+n_c\|g_T\|$	$\|p\|n_k+\|g\|$
U-ABE	$2n_k+n_k\|p\|$	$4n_c+\|p\|$	$\|p\|+(n_k+1)\|g_T\|+n_c\|g\|$	$(\|g_T\|+1)n_c+(n_c+1)\|p\|$

5.2 实验分析

实验平台为 64 bit windows 操作系统，Intel®Core(TM) i5-4570 CPU 3.20GHz、内存 8.00GB，实验代码基于 PBC 进行修改与编写，使用 A 类超奇异曲线 $E(F_q)$：$y^2=x^3+x$，群 G 是 $E(F_q)$的子群，群 G 的阶为 160 bit，基域为 58 bit.

本次实验从 4 个方面展开：加密时间、私钥生成开销、检索时间、解密时间，分别测试属性数量、关键字数量与时间开销的关系.

5.2.1 加密时间

图 2 是 U-ABE 方案与文献[8]、文献[18]、ABKE-UR、AD-KP-ABE 的加密时间对比图，经过分析，U-ABE 方案优于其他三个方案，但劣于 AD-KP-ABE 的方案，随着访问策略的增加，U-ABE 方案的加密时间逐渐与 ABKE-UR 方案的加密时间相同．这是由于 U-ABE 方案中的访问策略是双向访问策略，而文献 ABKS-UR 的方案的访问策略是单向的.

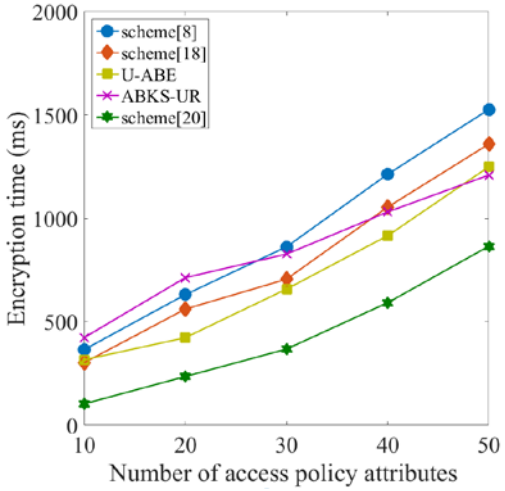


Fig. 2 comparison of encryption time experiment

图 2 加密时间实验对比

5.2.2 私钥生成开销

图 3 是 U-ABE 方案与文献[8]、文献[18]、ABKE-UR、AD-KP-ABE 的私钥生成开销对比图，从图中可以看出，随着用户提交的属性数量的增加，私钥的生成时间呈线性递增．U-ABE 方案的私钥生成是通过哈希运算以及指数运算的方式，相比其他四个方案，U-ABE 方案拥有更高的计算效率

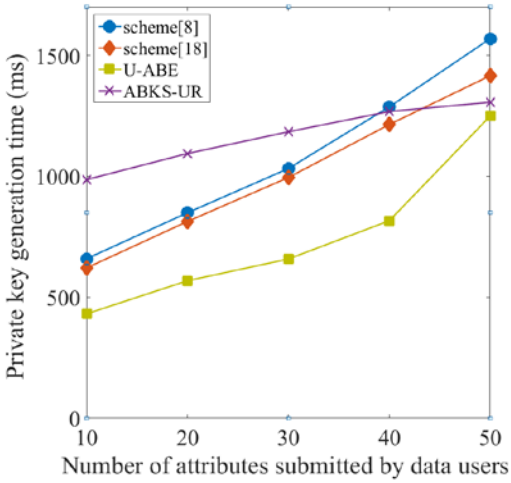


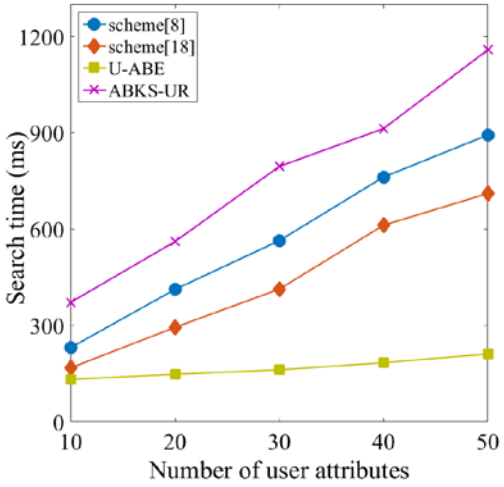
Fig3 comparison of private key overhead experiments

图 3 私钥开销实验对比

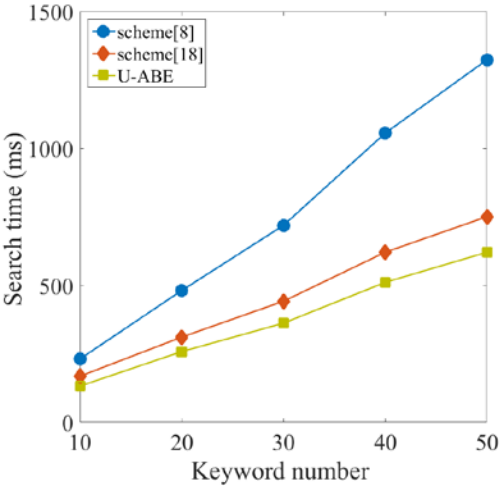
5.2.3 检索时间

图 4 是 U-ABE 方案与文献[8]、文献[18]、ABKE-UR 的检索开销对比实验，图(a)中的对比实验是用户私钥中的属性数量对检索时间的影响，同时设定关键字为 10，由于 U-ABE 方案的属性匹配是以集合的形式匹配，时间开销大大小于其他四个方案．图(b)中的实验对比是用户提交的关键字对检索时间的影响，同时设定用户属性为 10，从图中可以看出，随着关键字的增加，检索时间依然是呈现线性递增．U-ABE 方案虽然采用加入随机数计算陷门，构成了不可识别的陷门，但是由于在陷门的构建过程中只采用了一次双线性计算和一次指数运算，计算量相比其他三个方案来说要小。所以计算时间并没有因此

而增加.



（a）Number of attributes and retrieval time



（b）Keyword number and retrieval time

Fig4 comparison of retrieval time experiments

图 4 检索时间实验对比

5.2.4 解密时间

图 5 是 U-ABE 方案与文献[8]、文献[18]、AD-KP-ABE 的解密时间对比实验，从图中可以看出，解密时间随着用户私钥中的属性数量的增加而增加．经过分析，U-ABE 方案在解密时间上对文献[8]与文献[18]的方案有明显的优势，当用户私钥中的属性数量达到 50 时，U-ABE 方案的解密时间不到 1s，而文献[8]方案的时间已经近乎 2s．U-ABE 方案中的解密时间会随着私钥中属性数量的增加而增加，其原因主要是因为解密参数的计算，但是由于解密参数只是乘法运算，解密时间膨胀率低．

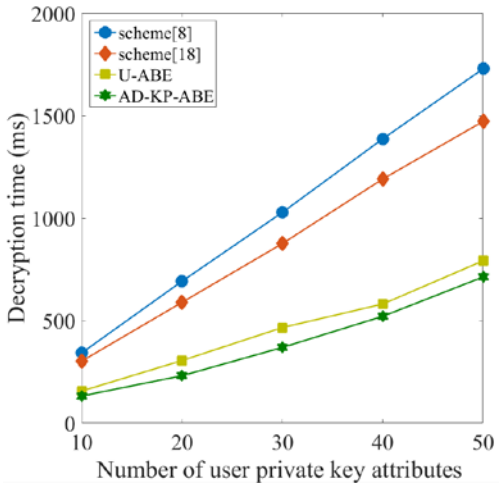


Fig5 comparison of decryption time experiment

图 5 解密时间实验对比

6 结束语

本文提出一种陷门不可识别的密文检索方案(U-ABE)．该方案通过引入拒绝访问策略，实现对访问属性的灵活控制，同时也可以实现双向撤销．由于该方案中，访问策略并没有嵌入到密文之中，可以通过访问策略的修改，完成灵活的属性撤销．该方案还引入了属性表格的机制，通过可靠的属性权威，制造坐标随机的属性表格，用户与拥有者都是以这个表格为基础进行属性与策略上的匹配，减少了匹配的计算时间，定时更换表格版本，提高安全性．该方案利用双线性对的双线性，引入随机数，构造出不可识别的陷门，实现了相同关键字每次加密结果都不同，保证了关键字的隐私．文中对方案做了安全性分析，证明得到方案是安全的，同时进行了详细的实验分析，实验证明方案在提高了安全性的同时也拥有较好的效率．未来的工作将在属性权威可信问题、精度与效率方面改进本文方案，并深入研究陷门安全问题，使其拥有更高的安全性．

参考文献

[1]. D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. IEEE Symposium on Security and Privacy (S&P 2000), pp. 44-55, 2000.

[2]. D. Boneh, G. Di Crescenzo, R. Ostrovsky, et al, “Public key encryption with keyword search,” in Proc. Advances in Cryptology-Eurocrypt 2004 (Eurocrypt’04), pp. 506-522, 2004.

[3]. Fang L, Susilo W, Ge C, et al. Public key encryption with keyword search secure against keyword guessing attacks without random oracle[J]. Information Sciences An International Journal, 2017, 238(7):221-241.

[4]. Shao Z Y, Yang B. On security against the server in designated tester public key encryption with keyword search[J]. Information Processing Letters, 2015, 115(8):1757-1761.

[5]. Sahai A, Waters B. Fuzzy Identity-Based Encryption[C]// International Conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag, 2005:457-473.

[6]. Bethencourt J, Sahai A, Waters B. Ciphertext-Policy Attribute-Based Encryption[C]// IEEE Symposium on Security and Privacy. IEEE Computer Society, 2007:321-334.

[7]. Pirretti M, Traynor P, Mcdaniel P, et al. Secure attribute-based systems[C]// IOS Press, 2006:1717-18.

[8]. Hur J, Noh D K. Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems[J]. IEEE Transactions on Parallel & Distributed Systems, 2011, 22(7):814-821.

[9]. Li J, Shi Y, Zhang Y. Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage[J].International Journal of Communication Systems, 2015, 30(1).

[10]. Ma H, Dong E, Liu Z, et al. Privacy-Preserving Multi-authority Ciphertext-Policy Attribute-Based Encryption with Revocation[C]// International Conference on Broadband and Wireless Computing, Communication and Applications. 2018:811-820.

[11]. Yang K, Jia X, Ren K. Attribute-based fine-grained access control with efficient revocation in cloud storage systems[C]// ACM Sigsac Symposium on Information, Computer and Communications Security. ACM, 2013:523-528..

[12]. Zu L, Liu Z, Li J. New Ciphertext-Policy Attribute-Based Encryption with Efficient Revocation[C]// IEEE International Conference on Computer and Information Technology. IEEE, 2014:281-287.

[13]. Sun W, Yu S, Lou W, et al. Protecting Your Right: Verifiable Attribute-based Keyword Search with Fine-grainedOwner-enforced Search Authorization in the Cloud[J]. IEEE Transactions on Parallel & Distributed Systems, 2016, 27(4):1187-1198.

[14]. Cui H, Deng R H, Liu J K, et al. Attribute-Based Encryption with Expressive and Authorized Keyword Search[C]// Australasian Conference on Information Security and Privacy. Springer, Cham, 2017:106-86.

[15]. Xue K, Hong J, Xue Y, et al. CABE: A New Comparable Attribute-Based Encryption Construction with 0-Encoding and 1-Encoding[J]. IEEE Transactions on Computers, 2017, PP(1717):14171-1503.

[16]. Chen Dongdong,Cao Zhenfu,Dong Xiaolei. Online/Offline Ciphertext-Policy Attribute-Based Searchable Encryption[J]. Journal of Computer Research and Development, 2016, 53(10): 2365-2375.

[17]. Zhao Y, Ren M, Jiang S, et al. An efficient and revocable storage CP-ABE scheme in the cloud computing[J]. Computing, 2018:1-25.

[18]. Qian H, Li J, Zhang Y, et al. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation[J]. International Journal of Information Security, 2015, 14(6):487-4177.

[19]. Canard S, Phan D H, Pointcheval D, et al. A new technique for compacting ciphertext in multi-channel broadcast encryption and attribute-based encryption[J]. Theoretical Computer Science, 2018:51-72

[20]. Xue L, Yu Y, Li Y, et al. Efficient Attribute-based Encryption with Attribute Revocation for Assured Data Deletion[J]. Information Sciences, 2018:157-165

作者简介

Du Ruizhong, born in 1975. PhD, professor. His main research interests include network security, trusted computing and Network technology.

Tan Ailun, born in 1995. Master candidate. Her main research interests include network security, trusted computing and Network technology.

Tian Junfeng, born in 1964. PhD, professor, PhD supervisor. His main research interests include distributed computing, network security, network technology.